WHAT IS CLAIMED IS:

1. An apparatus for protecting a computer system, comprising:

a password controller coupled to said computer system, said password controller capable of receiving a password attempt and capable of operating a computer program to compare said password attempt with a stored password, wherein said stored password comprises a password segment and said password segment comprises:

an entry event comprising a predetermined entry signal;

a predetermined time interval following said entry event; and

a terminating signal following said predetermined time interval, said terminating signal marking the end of said password segment;

wherein said computer program is capable of allowing access to said computer system when a password segment of said password attempt matches said password segment of said stored password.

2. The apparatus as set forth in Claim 1 wherein said computer program is capable of comparing a time envelope of said stored password with a time envelope of a received password attempt, and capable of denying access to said computer system when said time envelope of said received password attempt does not match said time envelope of said stored password.

3. The apparatus as set forth in Claim 1 wherein said computer program compares said stored password with said password attempt received from an online connection to determine whether said password attempt from said online connection matches said stored password.

4. The apparatus as set forth in Claim 1 wherein said entry event comprises a predetermined combination of computer readable entry signals, wherein each computer readable entry signal comprises one of: a character, a symbol, and a number.

5. The apparatus as set forth in Claim 1 wherein said terminating signal is an entry event that follows said predetermined time interval.

6. The apparatus as set forth in Claim 3 wherein said computer program is capable of sending a signal to said online connection that indicates whether said password attempt received from said online connection matches said stored password.

7. The apparatus as set forth in Claim 6 wherein computer program is capable of waiting until a time delay period expires before sending said signal that indicates whether said password attempt received from said online connection matches said stored password.

8. The apparatus as set forth in Claim 7 wherein said time delay period is of variable duration.

9. The apparatus as set forth in Claim 1 wherein said stored password comprises at least one password segment comprising a predetermined time interval calculated by subtracting from the total time measured from the trailing edge of a first entry event to the trailing edge of a next second entry event the time required to read said next second entry event.

10. The apparatus as set forth in Claim 2 wherein said stored password further comprises a plurality of password segments wherein the total time of said plurality of password segments equals said time envelope of said stored password, within a predetermined deviation.

11. An apparatus for protecting a computer system, comprising:

a password controller coupled to said computer system, said password controller capable of receiving a password attempt and capable of operating a computer program to compare a time envelope of a received password attempt with a time envelope of a stored password, and capable of denying access to said computer system when said time envelope of said received password attempt does not match said time envelope of said stored password.

12. A method of protecting an computer system, comprising the steps of:

detecting an initial entry event of a password attempt;

determining whether a password segment of said password attempt matches a password segment of a stored password wherein said password segment comprises:

an entry event comprising a predetermined entry signal;

a predetermined time interval following said entry event; and

a terminating signal following said predetermined time interval, said terminating signal marking the end of said password segment; and

allowing access to said computer system when said password segment of said password attempt matches said password segment of said stored password.

13. The method as set forth in Claim 12 further comprising the step of:

calculating a time interval of said password segment of said password attempt by subtracting the time required to read a next second entry event from the total time measured from the trailing edge of a first entry event to the trailing edge of said next second entry event; and

determining whether said time interval of said password segment of said password attempt matches a time interval of said password segment of said stored password.

14. The method as set forth in Claim 13 further comprising the steps of:

waiting for a time delay period to expire after determining whether said password attempt matches said stored password; and

sending a signal that indicates whether said password attempt matches said stored password.

15. The method as set forth in Claim 14 wherein said time delay period is of variable duration.

16. The method as set forth in Claim 13 further comprising the step of:

determining whether said entry event of each said password segment of said password attempt matches a corresponding entry event of said password segment of said stored password.

17. The method as set forth in Claim 13 further comprising the step of:

determining whether said time interval of said password segment of said password attempt matches a corresponding time interval of each said password segment of said stored password.

18. The method as set forth in Claim 12 further comprising the step of:

comparing each entry signal in said entry event in said password segment of said password attempt with a corresponding entry signal in said entry event of said password segment of said stored password.

19. The method as set forth in Claim 12 further comprising the step of:

beginning the timing of said password segment of said password attempt at the trailing edge of one of a first entry event and first entry signal; and

concluding the timing of said password segment of said password attempt at the trailing edge of one of a next second entry event and next second entry signal.

20. A method of protecting an computer system comprising the steps of:

detecting an initial entry event of a password attempt;

comparing a password segment of said password attempt to a password segment of a stored password;

determining whether said password attempt matches said stored password;

waiting for a time delay period to expire after determining whether said password attempt matches said stored password; and

allowing access to said computer system when said password attempt matches said stored password.

21. The method as set forth in Claim 19 further comprising the steps of:

comparing a time envelope of said stored password to a time envelope of said password attempt;

determining whether a time interval of a password segment of said password attempt matches a corresponding time interval of said password segment of said stored password; and

calculating a time interval of said password segment of said password attempt by subtracting the time required to read a next second entry event from the total time measured from the trailing edge of a first entry event to the trailing edge of said next second entry event.

22. For use in a computer, computer executable process steps stored on a computer readable storage medium capable of protecting said computer, comprising the steps of:

detecting an initial entry event of a password attempt;

determining whether a password segment of said password attempt matches a password segment of a stored password wherein said password segment comprises:

an entry event comprising a predetermined entry signal;

a predetermined time interval following said entry event; and

a terminating signal following said predetermined time interval, said terminating signal marking the end of said password segment; and

allowing access to said computer system when said segment of said password attempt matches said password segment of said stored password.

23. The computer executable process steps stored on a computer readable storage medium, as set forth in Claim 22, further comprising the steps of:

calculating a time interval of said password segment of said password attempt by subtracting the time required to read a next second entry event from the total time measured from the trailing edge of a first entry event to the trailing edge of said next second entry event; and

determining whether said time interval of said password segment of said password attempt matches a time interval of said password segment of said stored password.

24. The computer executable process steps stored on a computer readable storage medium, as set forth in Claim 22 further comprising the steps of:

waiting for a time delay period to expire after determining whether said password attempt matches said stored password; and

sending a signal that indicates whether said password attempt matches said stored password.

25. The computer executable process steps stored on a computer readable storage medium, as set forth in Claim 22, further comprising the step of:

waiting an arbitrary and variable time delay period before sending said signal that indicates whether said password attempt signals matches said stored password.

26. The computer executable process steps stored on a computer readable storage medium, as set forth in Claim 22 further comprising the step of:

determining whether said entry event of each said password segment of said password attempt matches a corresponding entry event of said password segment of said stored password.

27. The computer executable process steps stored on a computer readable storage medium, as set forth in Claim 22 further comprising the step of:

determining whether said time interval of said password segment of said password attempt matches a corresponding time interval of each said password segment of said stored password.

28. The computer executable process steps stored on a computer readable storage medium, as set forth in Claim 21 further comprising the step of:

comparing each entry signal in said entry event in said password segment of said password attempt with a corresponding entry signal in said entry event of said password segment of said stored password.

29. The computer executable process steps stored on a computer readable storage medium, as set forth in Claim 22 further comprising the step of:

beginning the timing of said password segment of said password attempt at the trailing edge of one of a first entry event and first entry signal; and

concluding the timing of said password segment of said password attempt at the trailing edge of one of a next second entry event and next second entry signal.